

CLAIMS

What is claimed is:

- 1 1. A method of remotely detecting vulnerabilities on a local computer,
2 comprising:
3 a) installing an agent on a local computer;
4 b) receiving encrypted commands for executing a risk-assessment scan from a
5 remote computer utilizing a network;
6 c) decrypting the commands on the local computer utilizing the agent;
7 d) processing the commands on the local computer utilizing the agent; and
8 e) performing the risk-assessment scan on the local computer in accordance
9 with the processed commands to remotely detect local vulnerabilities on the
10 local computer.
- 1 2. The method as recited in claim 1, wherein the agent includes a plurality of
2 risk-assessment modules.
- 1 3. The method as recited in claim 2, wherein the commands execute the risk-
2 assessment modules in a specific manner that is configured at the remote
3 computer.
- 1 4. The method as recited in claim 2, wherein the risk-assessment modules are
2 selected for the agent based on specifications of the local computer.
- 1 5. The method as recited in claim 2, wherein the risk-assessment modules
2 include a STAT module for performing a stat system call on a file, a READ
3 module for reading a file, a REaddir module for returning contents of a
4 directory, a FIND module for locating a list of files based on a given
5 function, a GETPWENT module for retrieving an entry from a password

6 database, a GETGREN module for retrieving an entry from a group
7 database, a CHKSUM module for performing a checksum operation on a file,
8 and an EXEC module for executing a command.

1 6. The method as recited in claim 2, wherein the risk-assessment modules are
2 selected from the group consisting of a STAT module for performing a stat
3 system call on a file, a READ module for reading a file, a READDIR module
4 for returning contents of a directory, a FIND module for locating a list of
5 files based on a given function, a GETPWENT module for retrieving an
6 entry from a password database, a GETGREN module for retrieving an
7 entry from a group database, a CHKSUM module for performing a checksum
8 operation on a file, and an EXEC module for executing a command.

1 7. The method as recited in claim 1, wherein the commands each indicate at
2 least one of the risk-assessment modules.

1 8. The method as recited in claim 7, wherein the commands are processed by
2 extracting parameters associated with the commands, and executing the risk-
3 assessment modules indicated by the commands utilizing the associated
4 parameters.

1 9. The method as recited in claim 1, and further comprising transmitting results
2 of the risk-assessment scan from the local computer to the remote computer
3 utilizing the network.

1 10. The method as recited in claim 9, and further comprising receiving feedback
2 to the results from the remote computer utilizing the network.

1 11. The method as recited in claim 1, wherein the commands are decrypted
2 utilizing a shared key.

- 1 12. A computer program product of remotely detecting vulnerabilities on a local
2 computer, comprising:
3 a) computer code for installing an agent on a local computer;
4 b) computer code for receiving encrypted commands for executing a risk-
5 assessment scan from a remote computer utilizing a network;
6 c) computer code for decrypting the commands on the local computer utilizing
7 the agent;
8 d) computer code for processing the commands on the local computer utilizing
9 the agent; and
10 e) computer code for performing the risk-assessment scan on the local computer
11 in accordance with the processed commands to remotely detect local
12 vulnerabilities on the local computer.
- 1 13. The computer program product as recited in claim 12, wherein the agent
2 includes a plurality of risk-assessment modules.
- 1 14. The computer program product as recited in claim 13, wherein the
2 commands execute the risk-assessment modules in a specific manner that is
3 configured at the remote computer.
- 1 15. The computer program product as recited in claim 13, wherein the risk-
2 assessment modules are selected for the agent based on specifications of the
3 local computer.
- 1 16. The computer program product as recited in claim 13, wherein the risk-
2 assessment modules include a STAT module for performing a stat system
3 call on a file, a READ module for reading a file, a READDIR module for
4 returning contents of a directory, a FIND module for locating a list of files
5 based on a given function, a GETPWENT module for retrieving an entry
6 from a password database, a GETGREN module for retrieving an entry

7 from a group database, a CHKSUM module for performing a checksum
8 operation on a file, and an EXEC module for executing a command.

1 17. The computer program product as recited in claim 13, wherein the risk-
2 assessment modules are selected from the group consisting of a STAT
3 module for performing a stat system call on a file, a READ module for
4 reading a file, a READDIR module for returning contents of a directory, a
5 FIND module for locating a list of files based on a given function, a
6 GETPWENT module for retrieving an entry from a password database, a
7 GETGENT module for retrieving an entry from a group database, a
8 CHKSUM module for performing a checksum operation on a file, and an
9 EXEC module for executing a command.

1 18. The computer program product as recited in claim 12, wherein the
2 commands each indicate at least one of the risk-assessment modules.

1 19. The computer program product as recited in claim 18, wherein the
2 commands are processed by extracting parameters associated with the
3 commands, and executing the risk-assessment modules indicated by the
4 commands utilizing the associated parameters.

1 20. The computer program product as recited in claim 12, and further comprising
2 computer code for transmitting results of the risk-assessment scan from the
3 local computer to the remote computer utilizing the network.

1 21. The computer program product as recited in claim 20, and further comprising
2 computer code for receiving feedback to the results from the remote
3 computer utilizing the network.

1 22. The computer program product as recited in claim 12, wherein the
2 commands are decrypted utilizing a shared key.

- 1 25. A method of remotely detecting vulnerabilities from a remote computer,
2 comprising:
3 a) sending encrypted commands from a remote computer to an agent on a local
4 computer for executing a risk-assessment scan utilizing a network, the
5 commands adapted for being decrypted and processed on the local computer
6 utilizing the agent for performing the risk-assessment scan on the local

- 7 computer in accordance with the processed commands to remotely detect
8 local vulnerabilities on the local computer;
9 b) receiving results of the risk-assessment scan from the local computer
10 utilizing the network; and
11 c) transmitting feedback to the results from the remote computer to the local
12 computer utilizing the network.

- 1 26. A computer program product of remotely detecting vulnerabilities from a
2 remote computer, comprising:
3 a) computer code for sending encrypted commands from a remote computer to
4 an agent on a local computer for executing a risk-assessment scan utilizing a
5 network, the commands adapted for being decrypted and processed on the
6 local computer utilizing the agent for performing the risk-assessment scan on
7 the local computer in accordance with the processed commands to remotely
8 detect local vulnerabilities on the local computer;
9 b) computer code for receiving results of the risk-assessment scan from the
10 local computer utilizing the network; and
11 c) computer code for transmitting feedback to the results from the remote
12 computer to the local computer utilizing the network.

- 1 27. A method of remotely detecting vulnerabilities on a local computer,
2 comprising:
3 a) installing an agent on a local computer, the agent including a plurality of
4 risk-assessment modules selected based on at least one aspect of the
5 computer;
6 b) receiving encrypted commands for executing a risk-assessment scan from a
7 remote computer utilizing a network;
8 c) decrypting the commands on the local computer utilizing the agent;
9 d) authenticating the commands on the local computer utilizing the agent;

- 10 e) processing the commands on the local computer utilizing the agent, the
- 11 commands adapted to execute the risk-assessment modules in a specific
- 12 manner that is configured at the remote computer;
- 13 f) performing the risk-assessment scan on the local computer in accordance
- 14 with the processed commands to remotely detect local vulnerabilities on the
- 15 local computer;
- 16 g) transmitting results of the risk-assessment scan from the local computer to
- 17 the remote computer utilizing the network;
- 18 h) receiving feedback to the results from the remote computer utilizing the
- 19 network.

0905508-062904
T06290-0055080